CLAIMS

What is claimed is:

1. A method comprising:

obtaining data from a device for use as an input to a first cryptographic process;

creating an output of the first cryptographic process wherein the output is valid for a limited period of time; and

writing the output from the first cryptographic process to a storage location after the device is received by a user.

2. The method as set forth in claim 1, wherein the first cryptographic process is based on a time stamp.

3. The method as set forth in claim 1, wherein the data is obtained from the user.

4. The method as set forth in claim 3, wherein the data is entered with at least one of a biometric device, a keypad, and a microphone.

5. The method as set forth in claim 1, further comprising creating an output of a second cryptographic process, wherein the data is used as an input to the second cryptographic process.

6. The method as set forth in claim 5, wherein the second cryptographic process is based on a time stamp.

7. The method as set forth in claim 5, wherein the second cryptographic process is performed by at least one of a device, a point of sale (POS) terminal, a transaction privacy clearing house (TPCH), a vendor, and a financial processing system.

8. The method as set forth in claim 5, further comprising comparing at least one of the output of the first cryptographic process and the input to the first cryptographic process with at least one of the output of the second cryptographic process and the input to the second cryptographic process.

9. The method as set forth in claim 8, further comprising allowing a transaction based on the comparing.

10. The method as set forth in claim 8, further comprising preventing the transaction based on the comparing.

11. The method as set forth in claim 8, wherein the comparing occurs without providing an identity of the user.

12. The method as set forth in claim 1, wherein the device is configured with a limit on transactions to be authorized, the limit being at least one of:

limiting an amount of money to be spent in a given time period;

barring certain users from making certain types of transactions; and

barring certain types of transactions.

13. The method as set forth in claim 1, wherein the storage location is selected from the group consisting of a magnetic stripe, a magnetic stripe emulator, a bar code emulator, and a personal transaction card.

14. A computer readable medium containing executable computer program instructions, which when executed by a data processing system, cause the data processing system to perform a method comprising:

obtaining data from a device for use as an input to a first cryptographic process;

creating an output of the first cryptographic process wherein the output is valid for a limited period of time; and

writing the output from the first cryptographic process to a storage location after the device is received by a user.

15. The computer readable medium as set forth in claim 14, wherein the first cryptographic process is based on a time stamp.

16. The computer readable medium as set forth in claim 14, wherein the data is obtained from the user.

17. The computer readable medium as set forth in claim 16, wherein the data is entered with at least one of a biometric device, a keypad, and a microphone.

18. The computer readable medium as set forth in claim 14, the method further comprises creating an output of a second cryptographic process, wherein the data is used as an input to the second cryptographic process.

19. The computer readable medium as set forth in claim 18, wherein the second cryptographic process is based on a time stamp.

20. The computer readable medium as set forth in claim 18, wherein the second cryptographic process is performed by at least one of a device, a point of sale (POS) terminal, transaction privacy clearing house (TPCH), a vendor, and a financial processing system.

21. The computer readable medium as set forth in claim 18, the method further comprises comparing at least one of the output of the first cryptographic process and the input to the first cryptographic process and at least one of the

output of the second cryptographic process and the input to the second cryptographic process.

22. The computer readable medium as set forth in claim 21, the method further comprises allowing a transaction based on the comparing.

23. The computer readable medium as set forth in claim 21, the method further comprises preventing a transaction based on the comparing

24. The computer readable medium as set forth in claim 21, wherein the comparing occurs without providing an identity of the user.

25. The computer readable medium as set forth in claim 14, wherein the device is configured with a limit on transactions to be authorized, the limit being at least one of:

limiting an amount of money to be spent in a given time period;

barring certain users from making certain types of transactions; and

barring certain types of transactions.

26. The computer readable medium as set forth in claim 14, wherein the storage location is selected from the group consisting of a magnetic stripe, a magnetic stripe emulator, a bar code emulator, and a personal transaction card.

27. An apparatus comprising:

security logic used to perform a first cryptographic process wherein an input to the first cryptographic process results in an output of the first cryptographic process wherein the output is valid for a limited period of time; and

a device communicatively coupled with the security logic and configured to write the output of the first cryptographic process to a storage location after the device is received by a user.

28. The apparatus as set forth in claim 27, wherein the storage location is a magnetic stripe emulator.

29. The apparatus as set forth in claim 27, wherein the storage location is a bar code emulator.

30. The apparatus as set forth in claim 27, wherein the storage location is associated with a personal transaction card.

31. The apparatus as set forth in claim 30, wherein the storage location is a magnetic stripe.

32. The apparatus as set forth in claim 27, wherein the first cryptographic process is based on a time stamp.

33. The apparatus as set forth in claim 27, further comprising a user interface communicatively coupled with the security logic, wherein the input to the first cryptographic process comprises data entered from the user interface.

34. The apparatus as set forth in claim 33, wherein the user interface is at least one of a keypad, a biometric unit, and a microphone.

35. The apparatus as set forth in claim 27, wherein the security logic comprises logic that confirms an identification, the identification selected from the group consisting of a personal identification number (PIN) code, voice identification, DNA identification, and biometric data.

36. The apparatus as set forth in claim 27, wherein the device is configured with a limit on transactions to be authorized, the limit being at least one of:

limiting an amount of money to be spent in a given time period;

barring certain users from making certain types of transactions; and

barring certain types of transactions.

37. An apparatus comprising:

a transaction terminal configured to communicate with a device wherein an output of a first cryptographic process is written from the device to the transaction terminal and the first cryptographic

process and a second cryptographic process are used to validate a transaction.

38. The apparatus as set forth in claim 37, wherein the second cryptographic process to be performed by at least one of a transaction terminal, a financial processing system, a transaction privacy clearing house (TPCH), the device, and a vendor.

39. The apparatus as set forth in claim 37, wherein the transaction terminal is selected from the group consisting of a point of sale (POS) terminal, home computer system, bank automatic teller machine (ATM) terminal, digital television, internet appliance, and personal POS terminal.

40. The apparatus as set forth in claim 37, wherein the second cryptographic process is based on a time stamp.

41. The apparatus as set forth in claim 37, wherein a comparison of at least one of the output of the first cryptographic process and the input to the first cryptographic process with at least one of an output of the second cryptographic process and an input to the second cryptographic process allows a transaction if a result of the comparison is within a predetermined range.

42. The apparatus as set forth in claim 41, wherein the comparison occurs at the transaction terminal.

43. The apparatus as set forth in claim 41, wherein the comparison occurs without providing an identity of the user.

44. The apparatus as set forth in claim 37, wherein a comparison of at least one of the output of the first cryptographic process and the input to the first cryptographic process with at least one of an output of the second cryptographic process and an input to the second cryptographic process prevents a transaction.

45. The apparatus as set forth in claim 44, wherein the comparison occurs at the transaction terminal.

46. The apparatus as set forth in claim 44, wherein the comparison occurs without providing an identity of the user.

47. An apparatus comprising:

a transaction terminal configured to communicate with a personal transaction card wherein an output of a first cryptographic process is written from the personal transaction card to the transaction

terminal and the first cryptographic process and a second cryptographic process are used to validate a transaction.

48. The apparatus as set forth in claim 37, wherein the second cryptographic process to be performed by at least one of the transaction terminal, a financial processing system, a transaction privacy clearing house (TPCH), a device, and a vendor.

49. The apparatus as set forth in claim 47, wherein the transaction terminal is selected from the group consisting of a point of sale (POS) terminal, home computer system, bank automatic teller machine (ATM) terminal, digital television, internet appliance, and personal POS terminal.

50. The apparatus as set forth in claim 47, wherein the second cryptographic process is based on a time stamp.

51. The apparatus as set forth in claim 47, wherein a comparison of at least one of the output of the first cryptographic process and the input to the first cryptographic process with at least one of an output of the second cryptographic process and an input to the second cryptographic process allows a transaction if the comparison is within a predetermined range.

52. The apparatus as set forth in claim 51, wherein the comparison occurs at the transaction terminal.

53. The apparatus as set forth in claim 51, wherein the comparison occurs without providing an identity of the user.

54. The apparatus as set forth in claim 47, wherein a comparison of at least one of the output of the first cryptographic process and the input to the first cryptographic process with at least one of an output of the second cryptographic process and an input to the second cryptographic process prevents a transaction.

55. The apparatus as set forth in claim 54, wherein the comparison occurs at the transaction terminal.

56. The apparatus as set forth in claim 54, wherein the comparison occurs without providing an identity of the user.

57. The apparatus as set forth in claim 47, wherein the device is configured with a limit on transactions to be authorized, the limit being at least one of:

limiting an amount of money to be spent in a given time period;

barring certain users from making certain types of transactions; and

barring certain types of transactions.